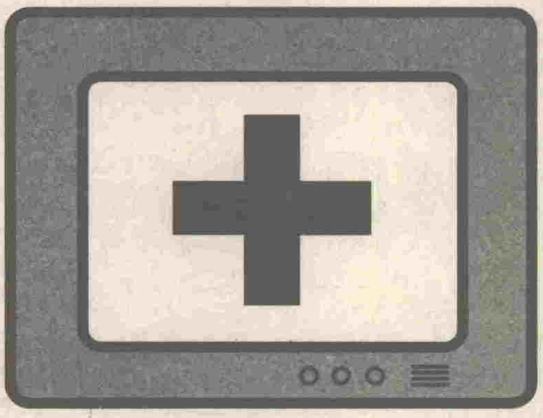
INTERNET

กองบรรณาธิการ

รักษาความปลอดภัยพีซี : ขณะใช้อินเทอร์เน็ต



เรื่องราวการป้องกันเบื้องต้นเพื่อป้องกันภัยเมื่อใช้คอมพิวเตอร์เชื่อมต่อกับอินเทอร์เน็ต

เรื่องราวของการใช้อินเทอร์เน็ตนอกจากต้องหาวิธีการใช้งานให้คุ้มค่าแล้ว วันนี้สิ่งที่ต้องคำนึงถึงคงจะไม่พ้นเรื่องราวของระบบการรักษาความปลอดภัย ใช้อินเทอร์เน็ตเราต้องเกี่ยวข้องกับระบบปฏิบัติการ อินเทอร์เน็ตจะใช้งานได้อย่างปลอดภัยหรือไม่ระบบปฏิบัติการไม่ว่าจะเป็นวินโดวส์ 95/98 ยูนิกซ์ หรือวินโดวส์เอ็นที

ระบบการรักษาความปลอดภัยเป็นประเด็นหลักอีกประการหนึ่งที่ผู้ใช้อินเทอร์เน็ตไม่ควรมองข้าม อินเทอร์เน็ตในวันนี้ไม่มีขอบเขตการใช้งานที่แน่ชัด เราไม่สามารถไปตามจับใครได้ว่าเขาหรือคนหนึ่งคนใดแอบใช้ข้อมูลส่วนตัวของเราบ้าง ข้อมูลบัตรเครดิต รหัสส่วนตัว หรืออื่น ๆ

สำหรับบทความในตอนนี้จะเป็นเรื่องราวการป้องกันเบื้องต้นเพื่อป้องกันภัยเมื่อใช้ระบบคอมพิวเตอร์เชื่อมต่อกับอินเทอร์เน็ต ด้วยระบบปฏิบัติการวินโดวส์ทั้งเอ็นที 4.0 และ 95 รวมถึงระบบยูนิกซ์

ขอเน้นย้ำว่าเป็นการป้องกันเบื้องต้นเท่านั้น เพราะเป็นที่ทราบกันดีว่าความสามารถในการเจาะระบบของเหล่าผู้ใช้คอมพิวเตอร์ชั้นเซียนนั้นไร้ขีดจำกัด

ป้องกันระบบเมื่อใช้ Windows NT ต่อกับอินเทอร์เน็ต

ข้อควรปฏิบัติเบื้องต้นเพื่อให้การใช้วินโดวส์เอ็นทีเชื่อมต่อกับระบบอินเทอร์เน็ตได้อย่างสบายใจในระดับหนึ่ง เริ่มจากติดตั้งระบบวินโดวส์เอ็นที 4.0 ที่เลือกระบบที่ติดตั้งน้อยที่สุด เอาเป็นว่าติดตั้งเฉพาะส่วนที่จำเป็นต้องใช้งานเท่านั้น ถ้าหากติดตั้งระบบที่เกี่ยวข้องกับการใช้งานและการบริการเครือข่ายมากเท่าไหร่ ก็เท่ากับว่าเปิดช่องทางให้สามารถเข้าถึงระบบของเราจากภายนอกได้ง่าย ระบบไฟล์ควรจะใช้แบบ NTFS (Windows NT Files System) ถ้าหากระบบยังเป็นแบบ FAT คงต้องแนะนำว่าให้แปลงเป็นแบบ NTFS ติดตั้ง Service Pack ล่าสุดเท่าที่จะหาได้ ตั้งแต่ SP 3 ขึ้นไป จะช่วยในการแก้ข้อผิดพลาดทางด้านระบบการรักษาความปลอดภัย

รักษาบัญชีรายชื่อผู้ใช้ให้ปลอดภัย

- เปลี่ยนชื่อและรหัสผ่านของผู้ดูแลเครือข่ายและระบบ ไม่จำเป็นต้องใช้ชื่อ Administrator เพราะชื่อนี้เป็นที่ล่อตาล่อใจบรรดานักเจาะระบบทั้งหลาย
- สำหรับ Administrator บัญชีนี้หลังจากเปลี่ยนแล้วให้สามารถทำงานหรือได้น้อยที่สุดหรือแทบจะทำอะไรไม่ได้เลย
- จำกัดจำนวนผู้ใช้ในกลุ่ม Administrator ยิ่งมีจำนวนยูสเซอร์มากยิ่งจะเป็นเป้าหมายสำหรับการถูกแฮกได้มากเท่านั้น

● สำหรับ Guest บัญชีนี้ปิดไปเลยยิ่งดี แต่ถ้าจำเป็นต้องมีรหัสผ่านสำหรับบัญชี Guest ด้วย

● การกำหนดรหัสผ่านต้องใช้ตัวอักษรผสมกับสัญลักษณ์พิเศษไม่ต่ำกว่า 6 ตัวอักษร

● มีบัญชีสำหรับการล็อกและปลดล็อกสำหรับใช้กับกลุ่มผู้ใช้

จัดเก็บฐานข้อมูลเกี่ยวกับผู้ใช้ ป้องกันค่ารีจิสทรีของระบบ ปิดการเข้าถึงระบบผ่านทางอินเทอร์เน็ตหรือเครือข่ายภายนอก ปิดบริการแจ้งข้อความอัตโนมัติ ปิดบริการ Dcom ถ้าหากติดตั้งระบบ IIS ต้องแน่ใจว่าได้ติดตั้งและรัน Service Pack ตัวล่าสุด ถ้าไม่ได้ใช้หรือบริการ FTP ทางที่ดีและปลอดภัยต้องปิดบริการ อย่าตั้งค่าให้วินโดวส์ล็อกออนสู่ระบบแบบอัตโนมัติ ไม่ต้องติดตั้ง Simple TCP/IP Service ยกเลิกการใช้ WINS Client

ป้องกันระบบเมื่อใช้ Windows 95

คำแนะนำเบื้องต้นที่จะป้องกันภัยจากการใช้อินเทอร์เน็ตด้วยวินโดวส์ 95 เราคงไม่สามารถป้องกันการลักลอบใช้ข้อมูลหรือใช้โปรแกรมถ้าหากผู้ใช้ไม่ได้เข้ามาทางเครือข่าย ดังนั้นทางป้องกันสำหรับการลักลอบใช้งานเครื่องคงเป็นเรื่องของระบบการรักษาความปลอดภัยโดยรวมที่ต้องหาทางป้องกันเอาเอง แต่สำหรับการป้องกันการเข้าถึงหรือเรียกใช้ข้อมูลผ่านเครือข่ายโดยเฉพาะอินเทอร์เน็ต เริ่มจาก ติดตั้ง Service Pack 1 วิธีการดูว่าเครื่องของเราได้ติดตั้ง SP1 ไปหรือยังดูได้จากการแสดงเวอร์ชันในแถบ General ของไอคอนของ System (ใน Control Panel) และต้องไม่แชร์ไฟล์ พรินเตอร์ และล็อกออฟทุกครั้งเมื่อต้องไปทำธุระเป็นเวลานาน มีการใช้รหัสผ่านสำหรับโปรแกรมรักษาจอภาพ (Screen Saver) สุดท้ายอย่ารันโปรแกรมที่เราไม่รู้ที่มาที่ไป เช่น จากอีเมล์ เว็บ หรือมีใครบางคนส่งมาให้

สำหรับวินโดวส์ 98 ค่อนข้างจะมีระบบรักษาความปลอดภัยที่ดี เช่น ไม่สามารถ NUKE เข้าทางพอร์ต 139 ดังนั้นผู้ที่ใช้ ICQ สบายใจได้ครับ

ป้องกันระบบเมื่อใช้ UNIX

สำหรับระบบยูนิกซ์ที่ทำงานบนเครื่องหลายแพลตฟอร์มนั้นมีหลักง่าย ๆ ในการป้องกันโดยรวมสำหรับผู้ดูแลระบบและการติดตั้งระบบดังนี้ ในการให้บริการสำหรับเครือข่าย ให้เซอร์ฟเวอร์บริการลูกข่ายน้อยที่สุดเท่าที่จำเป็น เช่น เครื่องเป็นเว็บเซอร์ฟเวอร์ ก็ไม่ต้องเปิดบริการ FTP หรือเปิดเป็นเมล์เซอร์ฟเวอร์ ติดตามข่าวคราวและการแจ้งเกี่ยวกับระบบการรักษาความปลอดภัยจากผู้แทนจำหน่าย มีการแพตช์ระบบยูนิกซ์ด้วยซอฟต์แวร์ตัวล่าสุดจากผู้แทนจำหน่าย และสุดท้ายรหัสผ่านของ Root ต้องรักษาให้ดี ต้องเป็นรหัสผ่านที่แกะยาก

ส่งท้าย

สำหรับตอนหน้าจะเป็นเรื่องราวของความปลอดภัยในการใช้อินเทอร์เน็ตสำหรับธุรกิจและชีวิตประจำวัน ที่ต้องนำเรื่องราวของระบบการรักษาความปลอดภัยมากล่าวถึงเป็นเพราะว่าระยะนี้ในหลายองค์กรธุรกิจเริ่มจะทำธุรกรรมทางการค้าผ่านอินเทอร์เน็ตกันมากขึ้น เช่น The Values ได้มีการเปิดตัว Value e-Business เพื่อบริการลูกค้า และทางภาครัฐได้เห็นความสำคัญ แต่สิ่งที่เราท่านทุกคนต้องตระหนักคือมาตรการรักษาความปลอดภัย